



Registre des activités de traitement des données personnelles

(Article 31 du règlement 2018/1725)

Version du : 09/12/2025

Numéro de référence : 194

Surveillance de la cybersécurité et la réponse aux incidents

Domaine d'activité : Activité administrative

Coordonnées

<i>Responsable du traitement ou Responsables conjoints du traitement :</i>	Direction des technologies de l'information, Cour de Justice de l'Union européenne, L-2925 Luxembourg	<i>Délégué à la protection des données :</i> Contact DataProtectionOfficer@curia.europa.eu
<i>Coordonnées de contact :</i>	DTI-data-controller@curia.europa.eu	
<i>Service traitant :</i>	Sécurité des systèmes d'information	
<i>Sous-traitant :</i>	Consultants externes, prestataire de services institutionnel de l'UE et le fournisseur de la Plateforme de	

Accessible au public

détection et réponse étendue (XDR).

Description du traitement

1) <i>Finalité du traitement</i>	Permettre à l'institution de détecter, de prévenir et de répondre efficacement aux incidents de sécurité informatique, conformément au Règlement (UE/Euratom) 2023/2841 établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union.
2) <i>Description du traitement</i>	Traitements requis dans le cadre de la gestion des incidents, des audits ou des évaluations de sécurité, de la détection d'intrusion et de la gestion des événements de sécurité.

<i>Catégorie de personnes concernées</i>	<i>Catégorie de données concernées</i>	<i>Durée de conservation des données</i>
- Tous les membres du personnel de l'institution, leurs interlocuteurs, les consultants externes et les visiteurs accédant à l'infrastructure informatique de la Cour (par exemple le WIFI). -Personnes disposant de biens informatiques de la Cour.	-Tout fichier suspect comme les fichiers joints à un courriel suspecté de contenir des logiciels malveillants ou des virus.	Les informations des systèmes de sécurité utilisées pour la détection des menaces sont conservées pendant une durée nécessaire pour réaliser des analyses et créer des liens entre différents évènements. Les données concernant un incident sont conservées pendant 5 ans à
	-Nom adresse de courrier électronique, numéro de téléphone, poste occupé.	
	-Données techniques (adresse IP, adresse de la machine, et autres données techniques).	

Accessible au public

	-Données relatives au trafic Internet, réseau et autres données relatives à une personne identifiée (matériel utilisé, URL, adresse IP, login, expéditeur, destinataire sujet, date, heure, lieu, nom de l'application, volume du fichier, nom du fichier, volume des données).	compter de la clôture de la procédure relative à l'évènement ayant initié leur collecte.
--	---	--

3) <i>Destinataires</i>	
a) <i>Au sein de l'institution</i>	Le Responsable de la Sécurité des Systèmes d'Information, les membres de l'équipe du service de Sécurité des systèmes d'information et de l'équipe de réponse aux incidents de sécurité et le Directeur de la DTI.
b) <i>À l'extérieur de l'institution</i>	Si l'assistance d'un prestataire de services institutionnels de l'UE s'avère nécessaire, les données d'incident ou de la surveillance de la sécurité peuvent être transmises à ce prestataire, dont le personnel doit respecter les mêmes exigences de confidentialité et de protection des données que les nôtres. Fournisseur de la Plateforme de détection et réponse étendue (XDR) dans certaines conditions.
4) <i>Transfert à un pays tiers ou une organisation internationale</i>	Néant
5) <i>Mesures de sécurité</i>	Plusieurs mesures de sécurité sont dérivées des règlements et normes suivantes :

Accessible au public

	le règlement 2023/2841 pour la cybersécurité, les normes ISO/IEC 27002 et ISO/IEC 27005 pour l'analyse des risques et le règlement 2018/1725 pour la DPIA.
6) <i>Notice d'information</i>	La notice d'information concernant ce traitement est accessible sur le site Intranet et sur le site de la Cour.
7) <i>Limitations des droits</i>	Néant